CLAIMS

What is claimed is:

1. In a computer network, apparatus for mapping data between different domains comprising:

a communication module for establishing a communication connection between a sender of one domain and a receiver in a different domain;

a mapping module coupled to the communication module for mapping working data of the one domain to working data of the different domain, the working data having an identifier portion and a research data portion, the mapping module mapping between the identifier portion of the working data in the one domain to the identifier portion of the working data in the different domain.

2. Apparatus as claimed in Claim 1 wherein the research data portion of the working data includes personal data of individuals.

3. Apparatus as claimed in Claim 1 wherein the communication connection is a secure communication channel formed by the communication module (i) authenticating the sender and receiver, resulting in an authorized sender and authorized receiver, and (ii) encrypting working data transmitted over the channel.

4. Apparatus as claimed in Claim 3 wherein the mapping module employs encryption in the mapping of working data in the domain to working data in the different domain such that the working data transmitted to the authorized receiver is anonymous data.

5. Apparatus as claimed in Claim 1 further comprising a secret sharing module for controlling access to the apparatus.

6. Apparatus as claimed in Claim 5 wherein the secret sharing module controls access to the mapping module.

7. Apparatus as claimed in Claim 5 further comprising permanent storage means for storing data in a tamper-proof manner.

8. Apparatus as claimed in Claim 7 wherein the permanent storage means encrypts non-queried parts of the data, said encryption using an encryption key, and the secret sharing module storing the encryption key.

9. Apparatus as claimed in Claim 8 wherein the permanent storage means employs digital signatures on queried parts of the data to detect changes in data and thereby prevent tampering.

10. Apparatus as claimed in Claim 9 wherein each digital signature is formed from a message digest of a concatenation of the encryption key and data.

11. Apparatus as claimed in Claim 9 wherein the permanent storage means maintains a summary measure of stored data.

12. Apparatus as claimed in Claim 11 wherein said summary measure has a respective digital signature.

13. Apparatus as claimed in Claim 1 wherein the mapping module defines a mapping between any two domains by storing a mapping table having cross references between identifier portions of working data of the two domains.

14. Apparatus as claimed in Claim 13 wherein the mapping module stores a mapping table for plural domains, the mapping table being formed of (i) an index section and (ii) a working reference section, the index section indicating identifier portion of working data in a first subject domain and the working reference section indicating corresponding identifier portion in a second domain, the working reference being encrypted, such that the mapping module performs decryption on a part of the mapping table to determine usable cross reference of the working data.

15. Apparatus as claimed in Claim 1 wherein the mapping module maps working data among plural domains.

16. Apparatus as claimed in Claim 1 wherein the sender and receiver are respectively one of a software implementation and a human being.

17. Apparatus as claimed in Claim 1 wherein connection of the sender and receiver is in respective different sessions.

18. Apparatus as claimed in Claim 1 wherein the communication module further enables communication connection by a supervisor in addition to the sender and receiver.

19. Apparatus as claimed in Claim 18 wherein the communication connection by the supervisor enables remote operation of the apparatus by the supervisor.

20. A method for transferring and mapping data between different domains in a computer network, comprising the steps of:

transmitting working data from a sender in one domain to a receiver in a different domain, the working data having an identifier portion and a research data portion; and

mapping the working data of the one domain to working data of the different domain by mapping between the identifier portion of the working data in the one domain to the identifier portion of the working data in the different domain.

21. A method as claimed in Claim 20 wherein the step of transmitting includes including personal data of individuals in the research data portion.

22. A method as claimed in Claim 20 further comprising the step of establishing a secure communication connection between the sender and receiver, wherein said secure communication connection includes (i) authentication of the sender and receiver, resulting in an authorized sender and authorized receiver, and (ii) encryption of the transmitted working data.

23. A method as claimed in Claim 22 wherein the step of mapping includes encrypting such that the working data received by the authorized receiver is anonymous data.

24. A method as claimed in Claim 20 further comprising the step of controlling access within the computer network.

25. A method as claimed in Claim 20 further comprising the step of storing data in a tamper-proof manner in a permanent storage.

26. A method as claimed in Claim 25 wherein the step of storing includes encrypting non-queried parts of the data.

27. A method as claimed in Claim 26 wherein the step of storing further includes assigning a respective digital signature to each queried part of the data to enable detection of changes in the data and thereby prevent tampering.

28. A method as claimed in Claim 27 wherein the step of encrypting employs an encryption key, and

the step of assigning includes forming a digital signature from a message digest of a concatenation of data and the encryption key.

29. A method as claimed in Claim 27 wherein the step of storing working data includes maintaining a summary measure of stored data.

30. A method as claimed in Claim 29 wherein the step of maintaining a summary measure includes assigning a digital signature to the summary measure.

31. A method as claimed in Claim 20 wherein the step of mapping includes storing a mapping table having cross references between the identifier portions of the working data of the two domains.

32. A method as claimed in Claim 31 wherein the step of storing a mapping table includes storing a respective mapping table for each domain, each mapping table being formed of (i) an index section and (ii) a working reference section, the index section indicating identifier portion of working data in a first subject domain and the working reference section indicating corresponding identifier portion in a second subject domain, the working reference being encrypted; and

decrypting a part of the mapping table to determine usable cross reference of the working data.

33. A method as claimed in Claim 20 wherein the step of mapping includes mapping working data among plural domains.

34. A method as claimed in Claim 20 wherein the sender and receiver are respectively one of a software implementation and a human being.

35. A method as claimed in Claim 20 further comprising the step of establishing a communication connection between the sender and receiver where the sender is connected in one session and the receiver is connected in a different session.

36. A method as claimed in Claim 20 further comprising the step of connecting a supervisor to the computer network.

37. A method as claimed in Claim 36 further comprising the step of enabling remote control by the supervisor.

38. Apparatus as claimed in Claim 1 wherein the identifier portion of the working data includes identifiers from plural domains, the mapping module mapping multiple identifiers between multiple domains for each reasearch portion of the working data.

39. Apparatus as claimed in Claim 1 further comprising:

a secured container;

a computer system executing the communication module and the mapping module; and

a firewall coupled to the computer system, the computer system and firewall being housed by the secured container so as to provide tamper-proof hardware.